



9111-97

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2018-0002]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services-018 Immigration Biometric and Background Check (IBBC) System of Records

AGENCY: Department of Homeland Security

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security (DHS) is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the “Department of Homeland Security/U.S. Citizenship and Immigration Services-018 Immigration Biometric and Background Check System of Records” and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2018-0002 by one of the following methods:

- **Federal e-Rulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.

- Fax: 202-343-4010.
- Mail: Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2018-0002 for this notice. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Donald K. Hawkins, (202) 272-8030, USCIS.PrivacyCompliance@uscis.dhs.gov, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue N.W., Washington, D.C. 20529. For privacy questions please contact: Philip S. Kaplan, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the DHS U.S. Citizenship and Immigration Services (USCIS) has relied on two preexisting DHS/USCIS Privacy Act system of records notices (SORN) for the maintenance of USCIS biometric and background check records: “DHS/USCIS 002 Background Check Service,” 72 FR 31082 (June 5, 2007), and “DHS/USCIS-003 Biometric Storage System,” 72 FR 17172 (April 6, 2007). DHS plans to rescind these SORNs. Records covered under these preexisting SORNs will now be covered by one new system of

records named “DHS/USCIS-018 Immigration Biometric and Background Check System of Records” (IBBC). This SORN consolidates all USCIS records maintained on biometric and associated biographic information it collects pursuant to its mission to process and adjudicate immigration benefit requests and other immigration request forms (e.g., applications and petitions). The purpose of this system is to verify identity and conduct criminal and national security background checks in order to establish an individual’s eligibility for an immigration benefit or other request, and support domestic and international data sharing efforts. USCIS determines eligibility by capturing biometric and associated biographic data from benefit requestors, beneficiaries, and other categories of individuals to facilitate three key operational functions: (1) verify an individual’s identity; (2) conduct criminal and national security background checks; and (3) produce benefit cards/documents as a proof of benefit. Further, this system permits the sharing of information covered by this system between the United States and foreign partners to prevent terrorism, including terrorist travel; prevent serious crime and other threats to national security and public safety; and assist in the administration and enforcement of immigration laws.

A description of this consolidated system is further described in DHS/USCIS’s notice of a new Privacy Act systems of records published elsewhere in this *Federal Register*.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework under which Federal Government agencies collect, maintain, use, and disseminate individuals’ records. The Privacy Act applies to information that is

maintained in a “system of records.” A “system of records” is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

The Privacy Act allows government agencies to exempt certain records from the access and amendment subsection 552a(d) provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking and Final Rule to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/USCIS-018 Immigration Biometric and Background Check System of Records. Information in DHS/USCIS-018 Immigration Biometric and Background Check System of Records relates to official DHS national security, law enforcement, immigration, and intelligence activities. These exemptions are needed to protect ongoing investigations and law enforcement activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS’s ability to obtain information from third parties and other sources; and to safeguard classified information. Disclosure of information to

the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 is revised to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. Add at the end of appendix C to part 5, the following new paragraph “78”:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

78. The DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records covers electronic and paper records and will be used by DHS and its components. The DHS/USCIS-018 IBBC System of Records covers information held by DHS/USCIS in connection with its several and varied missions and functions, including, but not limited to, the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/USCIS-018 IBBC System of Records contains information that is collected by, on

behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, tribal, foreign, or international government agencies.

The Secretary of Homeland Security, pursuant to Secretary's delegation 15002 to the Director of USCIS to conduct certain law enforcement activities when necessary to protect the national security and public safety, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national

security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

- (b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. From subsection (d) (Amendment to Records) because permitting amendment of records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.
- (c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

- (d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.
- (e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.
- (f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.
- (g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

- (h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.
- (i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Philip S. Kaplan
Chief Privacy Officer,

Department of Homeland Security

[FR Doc. 2018-16137 Filed: 7/30/2018 8:45 am; Publication Date: 7/31/2018]